Detailed Security Assessment — itsecgames.com / 31.3.96.40

Report date: 2025-09-25
Below I use the actual tool outputs you pasted as evidence; I then identify vulnerabilities, explain impact, and give prioritized remediation steps (commands / config examples included).

---

1 — Evidence (tool outputs you provided)

Use these exact snippets as audit evidence.

WHOIS (domain registration)

```
Domain Name: ITSECGAMES.COM

Registrar: GoDaddy.com, LLC

Creation Date: 2012-05-21

Registry Expiry Date: 2027-05-21

Name Server: NS53.DOMAINCONTROL.COM

Name Server: NS54.DOMAINCONTROL.COM

DNSSEC: unsigned
```

Nmap (initial full-port scan)

```
Nmap scan report for itsecgames.com (31.3.96.40)

Host is up (0.15s latency).

PORT    STATE SERVICE

22/tcp  open  ssh

80/tcp  open  http

443/tcp open  https
```

Nmap (follow-up -sV -sC) — later scan was filtered

```
PORT    STATE    SERVICE VERSION

22/tcp  filtered ssh

80/tcp  filtered http

443/tcp filtered https
```

HTTP response headers (curl)

```
HTTP/1.1 200 OK

Date: Thu, 25 Sep 2025 20:21:38 GMT

Server: Apache

Expires: Sun, 19 Nov 1978 05:00:00 GMT

Cache-Control: no-cache, must-revalidate

X-Content-Type-Options: nosniff

Content-Language: en

X-Frame-Options: SAMEORIGIN

X-UA-Compatible: IE=edge

X-Generator: Drupal 7 (http://drupal.org)

Link: <http://31.3.96.40/>; rel="canonical",<http://31.3.96.40/>; rel="shortlink"

Content-Type: text/html; charset=utf-8
```

Nikto (HTTPS partial output)

```
+ SSL Info: Subject:  /CN=web.mmebvba.com

        Ciphers:  ECDHE-RSA-AES256-GCM-SHA384

        Issuer:   /CN=web.mmebvba.com

+ Server: Apache

+ /: The anti-clickjacking X-Frame-Options header is not present.

+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined.

+ /: The X-Content-Type-Options header is not set.

+ Root page / redirects to: https://www.mmebvba.com

+ Hostname '31.3.96.40' does not match certificate's names: web.mmebvba.com.

+ /modules.php?letter=... Post Nuke ... vulnerable to Cross Site Scripting (XSS).
```

Nikto (HTTP partial output)

```
+ Server: Apache

+ /: Drupal 7 was identified via the x-generator header.

+ /robots.txt: contains 68 entries which should be manually viewed.

+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.

+ /web.config: ASP config file is accessible.
+ /install.php, /UPGRADE.txt, /INSTALL.*.txt, /MAINTAINERS.txt, /LICENSE.txt return 200 OK
```

OpenSSL (TLS handshake)

```
verify error:num=18:self-signed certificate

verify error:num=10:certificate has expired

notAfter=May 22 09:07:54 2025 GMT

Certificate chain: self-signed CN=web.mmebvba.com

Protocol : TLSv1.2

Cipher : ECDHE-RSA-AES256-GCM-SHA384

Server public key is 2048 bit
```

---

2 — Summary of Vulnerabilities & Misconfigurations (high-level)

1. **Unsupported/End-of-life CMS:** Drupal 7 is exposed by the X-Generator: Drupal 7 header. Drupal 7 is no longer maintained (no further security patches after EOL) → *high* risk.
2. **Exposed installer/upgrade files and documentation** (/install.php, /UPGRADE.txt, /INSTALL*.txt, /MAINTAINERS.txt, /LICENSE.txt) → sensitive info disclosure; can aid exploit attempts. *critical/high*.
3. **Certificate problems:** self-signed certificate for web.mmebvba.com that is **expired (notAfter May 22 2025)** and does not match the target name (CN mismatch) → *high* (breaks TLS trust).
4. **Missing/partial HTTP security headers:** Strict-Transport-Security missing; inconsistent X-Content-Type-Options presence across scans; Content-Security-Policy missing → *medium*.
5. **Potential XSS vulnerability** flagged by Nikto (PostNuke module path /modules.php?...), and many robots.txt entries reveal attack-surface paths → *medium/high depending on verification*.
6. **Accessible web.config & disclosure of server technology (Apache + Drupal)** → *informational/medium* (fingerprinting aids attackers).
7. **Junk/unsupported HTTP methods accepted** → may reveal debugging endpoints or allow unsafe verbs; *low/medium*.
8. **SSH port observed earlier open (22)** — may be reachable from some IPs; later scans showed filtered, suggesting dynamic filtering/IPS — *medium* until hardened.

---

3 — Prioritized Findings (with evidence & impact)

Severity categories: **Critical, High, Medium, Low, Informational**

Critical

A. Drupal 7 (End-of-life) — Remote code execution & exploited module risk

- **Evidence:** X-Generator: Drupal 7 (curl/Nikto).
- **Impact:** Drupal 7 is EOL and has known critical RCE/SQLi/XSS exploits that are widely automated. Attackers will scan for Drupal 7 and attempt public exploits.
- **Why critical:** Unpatched CMS allows remote compromise of site and server.

High

B. Expired / self-signed / mismatched TLS certificate

- **Evidence:** OpenSSL shows verify error: certificate has expired and CN web.mmebvba.com (not itsecgames.com), and Nikto notes hostname mismatch.
- **Impact:** Browsers warn; clients may be vulnerable to MITM; automated security checks and external services will flag site as insecure.
- **Remediation:** Replace with valid CA certificate for itsecgames.com (Let's Encrypt or other CA).

C. Exposed installation & documentation files (install/UPGRADE/INSTALL.*)

- **Evidence:** Nikto: many installation/upgrade files returned HTTP 200.
- **Impact:** These files leak application structure, default configs, and can sometimes enable re-installation or downgrade attacks. Attackers use these to craft exploits.

Medium

D. Missing security headers (HSTS, CSP, X-Content-Type-Options inconsistent)

- **Evidence:** Nikto reported Strict-Transport-Security missing, X-Frame-Options sometimes missing; curl output omitted HSTS.
- **Impact:** Increased risk of clickjacking, MIME-based attacks, and failure to enforce HTTPS.

E. Potential XSS / module vulnerabilities

- **Evidence:** Nikto flagged a module URL "Post Nuke 0.7.2.3-Phoenix ... vulnerable to Cross Site Scripting (XSS)".
- **Impact:** If valid, this can lead to session theft, admin credential capture, or stored XSS exploitation.

F. Exposed /web.config and long robots.txt listing

- **Evidence:** Nikto found /web.config; robots.txt contains 68 entries.

- **Impact:** Information leakage; robots entries can point attackers to admin, install, backup paths.

Low / Informational

G. Server header and technology fingerprinting

- **Evidence:** Server: Apache, X-Generator: Drupal 7.
- **Impact:** Aids attackers in selecting exploits; recommend obfuscation.

H. SSH exposure / filtered behavior

- **Evidence:** Nmap first showed SSH open, later filtered.
- **Impact:** If SSH is accessible, it must be hardened (keys, limited IPs). Filtering indicates some protections exist — confirm expected access.

---

4 — Concrete Mitigations & Remediation .

Area	Basic Recommendation
SSL/TLS Certificate	Renew the site's SSL/TLS certificate with a trusted Certificate Authority to replace the expired, self-signed certificate.
Web Server Security Headers	Enable essential HTTP security headers such as **Strict-Transport-Security**, **X-Frame-Options**, and **X-Content-Type-Options** to strengthen browser-side protection.
Drupal CMS	Update Drupal to the latest supported version and apply all official security patches.
Exposed Files & Directories	Restrict access to sensitive files (e.g., install.php, upgrade guides) and ensure only necessary files are publicly accessible.
Firewall & Access Control	Maintain proper firewall rules to allow only required ports and services while blocking unauthorized scans.